Industry Advisory Council
Transition Study Group

Identity and Access Management

December 9, 2008

Industry Advisory Council

The Industry Advisory Council (IAC) is a non-profit, non-partisan organization dedicated to fostering improved communications and understanding between government and industry. Through its affiliation with the American Council for Technology (ACT), the Industry Advisory Council provides a forum for industry to collaborate with and advise government executives on IT issues.

The Industry Advisory Council in cooperation with ACT is a unique, public-private partnership dedicated to helping government use technology to serve the public. The purposes of the organization are to communicate, educate, inform and collaborate. ACT-IAC also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes.

ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of information technology. For membership and other information, visit the ACT-IAC website at **www.actgov.org.**

Disclaimer

This document has been prepared to provide information regarding a specific issue. This document does not – nor is it intended to – take a position on any specific course of action or proposal. This document does not – and is not intended to – endorse or recommend any specific technology, product or vendor. The views expressed in this document do not necessarily represent the official views of the individuals and organizations who participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

Further Information

For further information, contact the Industry Advisory Council at (703) 208-4800 or www.actgov.org.

Executive Summary: Identity and Access Management

The United Stated has always been resistant to a national identity card, with fears centering on Big Brother tracking citizen movements and activities. As a result, identification in the United States has relied on a patchwork of unrelated documents. The list is long and includes birth certificates, Social Security cards, driver's licenses, passports, federally issued immigration and travel-related documents to non-U.S. citizens, and identity documents for permanent residents, transportation workers, military personnel, government employees and contractors.

The computer age has multiplied the number and types of documents and databases, with electronic credentials and verification systems available for specific purposes. Yet with all the advancements, most of the documents have their own limitations and there is no universal or consistent business process or approach.

As we approach the end of the first decade of the 21st Century and face many daunting new challenges at home and abroad, it is time to develop a consistent framework for identification. The federal government has a unique role to play in creating such a national strategy for identity management - a complex task that will require sensitivity, a need for innovation and technical expertise, and an effort to build public support.

Such a strategy must be designed to protect individual privacy and ensure accuracy while accomplishing a number of major goals including reducing losses from identity theft and fraud, facilitating a greater ability to share information securely across organizational boundaries, and enhancing commerce, mobility and travel security.

This will require collaboration across the government, between governments, and between the government and the private sector. And it will involve extending efforts already underway to improve government identity and access management programs.

The new administration faces some major tasks. It must implement centralized identity management and a federated framework for federal government employees and contractors. It also must standardize identity credentialing systems for travel security, immigration control, and employment verification. There will be challenges to redefine privacy and related practices regarding collection and storage of data for identification and access control, but it can and should be done.

The Obama administration has an opportunity to make significant progress and build upon work already completed. The president-elect has promised to name a Chief Technology Officer and make technology an administration priority. Creating and implementing a national strategy for identity management should be at the top of the list.

Identity and Access Management

THE ISSUE

The federal government has a unique role to play in creating a national strategy for identity management to facilitate commerce, enhance mobility and travel security, and to promote privacy and accuracy in information security. Potential benefits include reduced loss from identity theft and fraud, greater ability to share information securely across organizational boundaries and the enhancement of on-line commerce.

In order to succeed, there must be collaboration across the government, between governments, and between the government and the private sector. This will involve extending efforts already underway to improve government identity and access management programs, and to resolve a number of underlying policy questions.

This white paper will focus on three related topics: identifying and understanding the challenges facing the United States in identity management; examining how best to complete the implementation of interoperable identity management for government employees and contractors; and looking at the key issues, challenges, and potential benefits related to identity management for first responders, international travel security, immigration, and employment verification.

Like most large enterprises facing dramatic growth in information technology and security threats, the federal government must focus on identity management to better protect existing assets and preserve public confidence.

One critical initiative resulting from Homeland Security Presidential Directive-12 (HSPD-12) is the adoption of Personal Identity Verification (PIV) standards for individuals accessing government facilities and systems. The objective of HSPD-12 is to enable security controls to interoperate across agency and system boundaries. The goal is laudable, but it is so rare that it has required a new set of technical and procedural standards from the National Institute for Standards and Technology (NIST). At present, many agencies have programs underway to issue credentials that are compliant with the HSPD-12/PIV standards for access to both information systems and physical facilities. Yet many do not have the infrastructure in place to fully enable interoperability between agencies. If this were supported by a layer of federation and governance on top of the basic identity technology, it could be a key enabler for sharing of information across agency boundaries for enhanced mission alignment. This would lead to lower costs and greater flexibility while at the same time increasing accountability and information security.

Better management of identities and user's permissions could be extended beyond the federal government workers and contractors to other populations where enhanced security is desired. This could include first responders, aviation and port workers, and others who need unescorted access to transportation facilities. It also could apply to those who require access to sensitive data such as law enforcement information or who need the ability to share that information among state and local governments. In addition, participants in various public entitlement programs such as Medicaid and those affected by immigration control are all good candidates for early adoption.

The knowledge gained from the HSPD-12 initiatives provides a solid base line for continued growth and success from the cooperative partnership of public and private sectors in deploying systems for identity management. We encourage the federal government to continue down that innovative path in partnership with the private sector.

THE CURRENT PICTURE

Identification in the United States today relies on a patchwork of documents from birth certificates and Social Security cards to driver's licenses and passports. The federal government issues immigration and travel-related documents to non-U.S. citizens, and a variety of identity documents for permanent residents, transportation workers, merchant mariners, military personnel, and other government employees and contractors. Electronic credentials and verification systems are available for particular purposes. All of the documents have their own limitations, and there is no universal or consistent business process or approach.

A description of the various documents most commonly used for credentialing and verification are presented in Appendix A.

THE PROBLEMS WE FACE

Perhaps the one issue that most constrains the effectiveness of today's identification management systems is lack of agreement on how to manage competing demands for identity protection and authentication capabilities with the legitimate need to protect privacy. Addressing privacy and other public policy concerns as well as promoting widespread public education on identity management are closely associated issues.

Different populations have different issues and needs for access management and authentication. Consumers are generally more receptive to new technology when receiving a benefit such as facilitated travel, reduced transaction cost, or to enable new service delivery methods. They are most comfortable when new technologies can be adopted voluntarily. But privacy concerns, compulsory participation, and federal government oversight have been cited as concerns with regard to the Real ID Act. This may help to explain why Real ID Act reforms have been resisted much more than elected RFID enablement of driver's licenses.

Prevention of identity fraud, assurance of transaction authentication for on-line commerce, streamlined mobility of people and assets with enhanced security, and protecting portable electronic health records, all can be promoted and secured more efficiently through an implementation of interoperable systems and distributed trust for identity management and authentication. The Malaysia model[1] is an example where the government multipurpose card is supported by a legal foundation that allows the identity management functions to be fully trusted. In the future, the ability to promote authentication for virtual work including multi-media content access control such as for secure video teleconferencing and secure video management may also be required.

In comparison, the beneficiary ID cards issued to Medicaid recipients lack effective verification and do not prevent duplicate enrollments, enrollment in multiple states, or usage by impostors to get treatment. The lack of effective verification contributes to fraud and abuse.

There also are problems with the E-Verify system. Employers and USCIS are at odds over the accuracy of the automated systems. There are currently over 80,000 employers using the system, and adding federal contractors would increase that number to over 250,000. A recent Inspector General Report indicated that Social Security records were erroneous in about 10 percent of the cases checked in the first half of 2007, although USCIS indicates independent audits show the system improving rapidly in its accuracy. It is unclear whether the system can withstand the major workload increases that will be required by wider employer participation if Congress were to make the program mandatory. There also are concerns about the scope of the automated system, whether the two federal agencies can cope with the workload and correct errors that occur. Lastly, the issue of verifying the identity of the worker presenting the document must be strengthened. Currently, a prospective employee who presents a Social Security number and claims to be a U.S. citizen by birth will not have any biometric identity check done. This creates a temptation for illegal workers to commit identity fraud, and leaves a significant hole in the verification system.

Another example of disparate systems is the DHS travel security programs that have overlapping requirements, but different approaches which are not interoperable. These include Global Entry, Domestic Registered Traveler, and international registered traveler initiatives.

[1] Outside the United States, some countries have national programs for multi-purpose identification systems. In Malaysia, for example, there is a government multipurpose card known as the MyKAD which is an electronic identification card protected by encryption. It contains a fingerprint biometric for identity verification and is designed as the platform for government and private sector applications. More than 20 million cards have been issued as ID cards and driver's licenses. The original 32k chip also had space for banks to store ATM card data and fast-toll information, and for consumers to utilize an e-purse for purchases up to $500. Today's 64k cards can accommodate digital certificates for protection of online identities in e-commerce and health records. This is an example of a government sponsored program providing a biometric platform and data to enable banks to protect transactions.

Federal security clearances represent another case where there is tremendous inefficiency and much waste due to repetitive efforts to clear employees sometimes within the same agency. The HSPD-12 issuance process requires the successful adjudication of, at minimum, a National Agency Check with Inquiries (NACI) background investigation. These investigations are conducted centrally by the FBI and Office of Personnel Management (OPM), but adjudications based on results are left to each federal agency. Historically, adjudication by one agency was meaningful only to that agency and was not necessarily accepted by any other. An employee transferring between organizations inside the Department of Justice such as from the FBI to DEA, for example, might be on the bench for a year before starting the new work duties while waiting for a new background investigation and adjudication. The HSPD-12 requirements underscore the need for standardization and reciprocity agreements that allow adjudications to be efficiently shared across agencies.

OPTIONS FOR IMPROVEMENT

Identity management is not just a public policy debate. It is also infused with pragmatic doubts about the empirical effectiveness of the technologies available such as biometrics and automated access control. Legitimate privacy concerns also abound when the public feels it cannot trust management practices in situations where data are standardized, federated, and aggregated, and enable monitoring of movement and behavior.

Addressing privacy and other public policy concerns as well as promoting widespread public education on identity management may be most effectively achieved by concentrating on specific functional benefits such as combating fraud and abuse, ensuring employment eligibility verification, and creating government security systems for access by employees and contractors. Federal policy also could encourage the identification systems that exist in the private marketplace today. Some of the private systems already provide better assurance of identity and trustworthiness than many government-issued ID cards.

One reform option that could gain public acceptance and protect government resources by combating fraud could be employed for Medicaid beneficiaries. Individuals and their family members could be requested to enroll biometrically, with the identity information placed in a centralized identity management system maintained by the Medicaid program. The beneficiary would be requested to go through a verification process using the credentials when requesting any Medicaid related services. Once the identity is confirmed, a verification check can be made against the patient's entitlements using the identity management system. This would guarantee a higher degree of identity assurance and address many types of beneficiary validation to reduce fraud and abuse. This approach is similar to what we see in the District of Columbia government One Card Program which is based on standards and interoperability requirements. The citizen card can also be used to store other biographic details like the address, the state where the beneficiary is enrolled and other relevant details. This will further increase the identity assurance level by allowing for various types of checks including enrollment status in other states to minimize the fraud and abuse incidents.

Since Medicaid programs are administered by the states, the enrollment process will be local to each of the states and will have its own procedures and systems in place. It would be critical that all the state based systems interact with each other or some central identity management system for better cross check verifications. In addition, the identity management systems would be required to interact with the Federal Fraud Investigation Database System (FIDS) to perform an integrity check on the individuals during the enrollment process and update the FIDS when fraud incidents occur.

In order to protect the privacy of the beneficiary, it would be necessary that all the policies, procedures and information systems that are part of the identity management system comply with HIPAA regulations including privacy and security rules.

There is much to learn from the Medicaid example about the value of personal identity verification that would have a centralized identity management information system managed through a governance process and containing a standards-based privacy and security safeguards to maintain public confidence.

These same principles apply to the other functional areas addressed in this paper and are some of the characteristics expected under the Real ID Act for driver's licenses. The vast majority of state governments are presently focused on upgrading their driver license processes and cards. Investments in upgrades of document authentication, enhanced card security, and detection technologies and penalties for ID theft will help improve the quality and the security of state drivers' licenses, and can help make state documents more effective for constituents in such areas as employment verification.[2] The federal government should support the innovation that is taking place by creating a positive partnership between the federal agencies with authority over credentialing, the governors, and state legislatures. Independent of the Real ID Act, the federal government should increase its financial commitment to helping the states improve their drivers' license programs.

The federal government through the HSPD-12 driven process and PIV standards has made important progress that should lead over time to increasing public confidence in these technologies. Soon we will see the results at many agencies with successful HSPD-12 implementations of new credentials that are compliant with the PIV standards for access to both

[2] For example, the new Montana license, which was issued beginning July 1, 2008, incorporates facial recognition, document authentication and highly secure card production mechanisms. Facial recognition is primarily used to prevent duplicate licenses from being issued to people. Optical technology helps to authenticate the documentation that people present to obtain licenses by comparing a "breeder document" against an extensive template library of passports, other state's driver's licenses, etc. The Montana DL is a PVC/polyester composite card with embedded overt, covert and forensic security features.

information systems and physical facilities. However, there is not yet the infrastructure in place to fully enable interoperability between agencies. If this were supported by a layer of federation and governance, it could be a key enabler for sharing of information across agency boundaries for enhanced mission alignment with lower costs and greater flexibility without compromising information security. Options for improvement associated with this concept, including further technical details and possible directions, appear in a companion paper entitled "Government Federated Identity Management".

ROADMAP FOR REFORM

The challenges and issues raised in this paper center on three related topics. It must be determined how best to complete the implementation of interoperable identity management for government employees and contractors, and how to deliver benefits related to identity management for employment verification, first responders, and for international traveler's security. It is also important to address identity management issues facing the United States, particularly where federal government action is appropriate. This includes emerging privacy policy issues such as the capture and use of biometric identifiers.

As supported in the companion paper, a natural next step is to implement centralized identity management and a federated framework for federal government employees and contractors. This may require additional analysis to quantify the benefits, costs, and potential agency responsibilities, and the establishment of a governance model. There are agencies with joint missions in the government that clearly are beneficiaries of an identity federation model.

One option could be to focus initially on enabling the National Response Framework. This is an overarching federal program administered by FEMA for dealing with emergencies and catastrophic events. Within the NRF, there are 15 Emergency Support Functions (ESF) with critical support services from, and primary oversight delegation to federal agencies including DOT, DOD, DHS, USDA, HHS, EPA, and DOJ. Each of these agencies interacts directly with other federal agencies, state, tribal, and municipal governments, emergency responders and private sector partners. The community that supports the NRF totals more than 16 million individual users, the vast majority of which will eventually be issued PIV cards.

The implementation of a consistent and interoperable identity management standard based on a national federation model for this community provides several important solutions. Emergency response communities can build secure on-demand collaboration environments to support incident preparation and data sharing as well as provide incident response communication during emergencies. By incubating this interoperable identification federation framework, an urgent need can be addressed immediately and gain traction in a landscape consisting of federal, state, tribal, municipal, and commercial partners.

Extending the federation to citizens for benefits and entitlement access via E-authentication should be on the agenda. The natural result would be to assimilate those citizens and a sizable number of federal employees and contractors affiliated with multiple agencies. This would result in an operational population that would include state, tribal, and municipal employees and contractors, and commercial partners across the country.

The adoption of this identity management federation model would firmly establish de facto standards around its conceptual and technological implementation. Upon widespread adoption, the federal government could elect to relinquish or delegate its oversight role in favor of federation partnership self-governance. There are numerous government agencies and commercial partners including Credential Service Providers (CSPs), financial institutions, credit agencies, and other entities managing identity data that may find it commercially viable to deliver identity management services. Government participation in standards setting organizations and in public sector and private sector partnerships would promote interoperability and encourage adoption.

A parallel effort should be undertaken to move towards the standardization of identity credentialing systems for travel security, immigration control, and employment verification. There also will be challenges to redefine privacy and related practices regarding collection and storage of biometric data for identification and access control. For example, facial images that could be used for biometric identification may be captured involuntarily by surveillance systems rather than through voluntary enrollment processes. There are currently no policy restrictions in place to prevent this from happening.

The realization of this vision builds upon the capabilities of HSPD-12 and leverages the existing hard-earned knowledge around federation management developed by groups such as Internet2/MACE and the InCommon Federation which are described in further detail in the companion paper. Ultimately, this model has the power to transform the broken and fragmented identity management landscape that exists today. It will provide tremendous benefits for government, commerce, and private citizens in terms of security, privacy, convenience, and efficiency in managing identity and identity attributes and in turn, in the provision of critical services.

APPENDIX A: THE CURRENT PICTURE

The array of documents issued for various credentialing and verification purposes are described below.

Social Security Cards

Social Security numbers issued for a specific citizen benefit are often used for unintended identification purposes, and sometimes with adverse consequences. The financial industry's use of the numbers for identification or account purposes, for example, has led to identity fraud and abuse.

Driver's Licenses

The driver's license is the most widely accepted identity document in the United States. This credential is routinely used to establish the holder's age and residence, to open a bank account, obtain credit, enter government buildings, board a plane, and provide access to a wide array of social privileges and services. In a country with limited passport issuance and an aversion to a national ID, the driver's license has become our nation's de facto citizen ID. As such, it is an extremely valuable document. A secure issuance process and an ability to authenticate the document are essential to combat such challenges as underage drinking and traffic safety, and to deter identity theft used to commit financial crimes, and to provide protections against potential terrorists. Driver's licenses have historically been loosely standardized through the efforts of the American Association of Motor Vehicle Administrators (AAMVA) and are functionally similar. Many include a means for electronic verification using a two-dimensional bar code bearing the same biographical data as the surface of the card. In September 2000, the states through the AAMVA voted to institute the Driver License Agreement (DLA) in an effort to establish standards that would ensure a "One Driver, One License, One Record" system. In 2004, a revised DLA was issued to and accepted by the states.

In the wake of 9/11 terrorist attacks, the federal government sought to expedite the pace of this change through legislation mandating federal standards to ensure a more secure driver's license that would protect citizens and enhance national security. The Real ID Act signed into law in 2005 imposed new requirements on the states to establish minimum standards for driver licenses or personal ID cards. Compliance costs over 10 years are estimated as high as $4.4 billion. The states believe that the Real ID Law is a large mandate that the federal government has not properly funded. Final regulations were issued to implement Real ID in 2008, with compliance deadlines beginning at the end of 2009.

The Real ID Act mandates that states strengthen their driver's license identity vetting process to comply with federal standards set by the Department of Homeland Security. It also calls for linking state databases for electronic information sharing, or risk that their documents will not be accepted for entrance at airports or federal courthouses.

To date, the Congress has only appropriated $90 million for specific state use to fulfill the general mandates of Real ID. The fiscal year 2009 appropriations process includes another $110M for states if the pending appropriations bills are passed.

The Department of Homeland Security also oversees a separate Real ID Demonstration Grant awards program that provides some additional funding. In fiscal year 2008, this program provided nearly $80 million in special grants to assist states in improving the security of state-issued driver's licenses and identification documents. These grants fund state-specific projects like improving the physical security of licenses, upgrading facility security, and modernizing document imaging and storage. Previously, $58 million in special grants had been allocated for state-specific implementation projects that facilitate Real ID compliance.

DHS is also supporting the development and testing of a verification hub that enables states to query federal and non-federal document-issuing authorities and verify applicant source documents. The hub will act as a central router to provide timely, accurate, and cost-effective verification to motor vehicle departments of an applicant's source documents. States will be able to seamlessly verify the identity, lawful status and Social Security number of an applicant through this common interface.

DHS has awarded $17 million to Missouri to lead the development of the verification hub. Four other states — Florida, Indiana, Nevada, and Wisconsin — will partner with Missouri for verification hub testing and implementation. Other states and territories will eventually connect to the verification hub and have the capability to verify applicants' source documents.

Passports

Only a minority of citizens have historically been issued passports because they were not until recently required to re-enter the U.S. when returning from foreign travel. New U.S. passports now contain an electronic chip with encrypted biographical data and a facial image of the traveler. The State Department also has begun to issue a Passport Card that may be used for travel in North America which contains a basic RFID identification capability to facilitate rapid passage through land ports of entry. State governments have been encouraged with federal grants to incorporate the same RFID technology in driver's licenses, and several have already chosen to do so.

Government IDs

Regarding government personnel, HSPD-12 requires a “mandatory, government-wide standard for secure and reliable forms of identification issued by the U. S. federal government to its employees and contractors.” This standard is embodied in Federal Information Processing Standard (FIPS) 201. However, the standards do not fully cover the interchange of data between agency systems, so agency adoption of HSPD-12/PIV compliant credentials have not been accompanied by cross-agency federation, data management and interoperability.

The HSPD-12 promise to improve the government's security posture rests on the use of two-factor (what you have/what you know) smartcard authentication, and the widespread deployment of a common identity authentication and access control infrastructure. The PIV electronic smartcard with biometrics in a standardized package has stimulated emergence of a practical commercially viable framework that is moving the market beyond vendor-specific solutions. It is now being adopted by state governments and the emergency responder community.

A derivative of the PIV standard has been adopted by the Department of Homeland Security for the Transportation Worker ID Credential (TWIC) required for private sector workers in order to have unescorted access to secure areas of transportation facilities. The Registered Traveler program uses iris and fingerprint recognition to verify the identity of travelers to access fast lanes at airport security screening checkpoints. These are issued by a number of private commercial service providers after a traveler's successful background check conducted by the Department of Homeland Security. Any registered traveler card can be used at checkpoints protected by different service providers because they are designed to be interoperable and share a common identity management model. This is an example of a public- private partnership and of interoperability via a secure framework.

Benefits eligibility is another area where identification systems requirements are useful. A few have been introduced including in the Medicaid health program for individuals and families with low incomes. Medicaid is jointly funded by the states and the federal government, and is managed by the states. The enrollment processes are managed by each state and beneficiaries are often issued an ID card to prove eligibility. Many states have implemented systems to verify eligibility (say for pharmacy benefits) but without identity verification. Some are moving toward a verifiable citizen card such as the District of Columbia government One Card Program which is based on standards and interoperability requirements.

Immigration IDs

One element of the contentious national immigration debate centers on verifying who is legally allowed to work. Legal workers include those who are U.S. citizens, lawful permanent residents commonly referred to as green card holders, and temporary residents who are authorized to work because of their immigration status. The government has developed an automated system to verify the employment eligibility of new hires. The United States Citizenship and Immigration Services system, now called E-Verify, is a joint effort between USCIS and the Social Security Administration. Participation of employers is voluntary, although several states have made it mandatory for companies in their states. In addition, the federal government has proposed rules that would make participation mandatory for federal contractors. E-Verify is a credential verification system, not an identity management system. A participating employer inspects a work authorization document presented by a prospective employee, and electronically forwards the document number to the E-Verify system. The document number is verified as a work eligible document either by SSA in the case of Social Security numbers or by USCIS.

There is also a major effort to increase security at the borders. This effort centers on travel documents used in the immigration systems and the interoperability of the automated systems.

The main government agencies involved includes the Department of Homeland Security and the Department of State. Since the creation of DHS, the two departments have made significant strides in the areas of information exchange and data interoperability. To enter the United States, foreign nationals are required to present identity documents which vary by immigration status. Many travelers may enter without a visa by presenting a passport from a visa-waiver country that meets international standards for a travel documents including biometric identifiers. Travelers from non-visa-waiver countries are required to have a visa issued by the State Department which must be preceded by a fingerprint-based background check. Mexican border crosser cards are visas in ID-card format that contain biographic indicators (photo, fingerprint and signature) using digital optical technology that tie the holder to the credential. Lawful permanent residents of the United States are required to present a Permanent Resident Card. These cards, produced by the USCIS, also contain biographic indicators (photo, fingerprint and signature) using optical technology that tie the holder to the credential. Biographical data from any of these credentials can be read through the main DHS automated system for immigration control at ports of entry, the US-VISIT system. US-VISIT is effective in tracking the entry of individuals into the United States by capturing each traveler’s fingerprints and photograph recorded as an entry record but currently does not have an exit control system to track departures.

The Private Sector

There are also private sector initiatives to address identity fraud that are centered largely in the financial community that have been initiated due to regulatory compliance, transaction protection and customer loyalty issues. Identity fraud receives continuous public attention, with headlines routinely describing dramatic losses of confidential customer information. Commercial data aggregators and credit bureaus, in some cases, have data fusion and biometric data capture programs to provide identity management and verification services. Global surveys of consumer attitudes confirm that a majority of respondents in every region are concerned about identity fraud and believe that there is a value for both individuals and private industry to achieve an interoperable system for identity verification.

GLOSSARY

Abriva - A free mobile identity management framework.

Authentication - The act of establishing or confirming that someone is who they claim to be. In an information technology sense this is confirming that someone is authentic typically by validating their credentials.

Authorization - A process of controlling access to information or resources only to those specifically permitted to use them.

Biological Identity - This is the concept of a belly-button. Every individual has one and only one biological identity. There are many attributes that are associated with and could be used in the aggregate to relate to the identity.

Credential - A defined collection of attributes that are asserted to meet the level required to validate the user and authenticate them.

Defense Cross-Credentialing Identification System (DCCIS) - infrastructure that provides a credentialing network for the Department of Defense.

E-Authentication - A federal government secure on-line access authentication initiative, see http://www.cio.gov/eauthentication/index.cfm for more information.

Electronic Identity - Digital identity, the representation of identity in terms of digital information or online identity.

Entitlement - Permission to access a resource. This may be based on a role, rules, or attributes.

Federated identity - Identity management with defined trust relations between independent principals.

Federation for Identity and Cross-Credentialing Systems (FIXs) - A coalition of commercial companies and not-for-profit organizations to establish interoperable identity and cross-credentialing compatible with PIV-aligned credentials and DCCIS.

Identity fraud (Identity Theft) - The deliberate appropriation of someone's identity without gaining that person's permission for criminal purposes.

Laws of identity – Concepts that define a unifying identity meta-system for online identity management.

Liberty Alliance — A consortium promoting federated identity management.

Security Assertion Markup Language (SAML) – SAML is a standard for exchanging XML-based authentication and authorization assertions between identity providers and service providers (assertion consumers).

Shibboleth (Internet2) - Shibboleth is an open source standards compliant federating software platform. Essentially it is a transport mechanism for digitally signed SAML assertions.

ACKNOWLEDGEMENTS

Writing Team
John Bird, BT Conferencing
Mark Cohn (Paper Lead), Unisys
Joe Cuddihy, McConnell International
Bill Harrod (Paper Lead), CA
Vivek Kumar, Softchoice Corporation
Dean Lindstrom, Cyberstorm
Kovelevenni Ramaswamy, QSSI

Transition Study Group Leadership
Mark Forman (Chair), KPMG
Roger Baker (Vice Chair)
Mary Ellen Condon, Booz Allen Hamilton
Judy Douglas, EDS, an HP Company
Dee Lee, Compusearch
Brien Lorenze, Deloitte
Leslie Steele, InterImage

ACT-IAC Staff
Kenneth Allen
Sarah Lindenau